UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/653,503	09/02/2003	Len L. Mizrah	AIDT 1005-1	3753

22470 7590 11/19/2007
HAYNES BEFFEL & WOLFELD LLP
P O BOX 366
HALF MOON BAY, CA 94019

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
11/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/653,503	**Applicant(s)** MIZRAH, LEN L.	
	Examiner Farid Homayounmehr	**Art Unit** 2132	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 23 October 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-4,6-11,13-18 and 20-30*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Continuation of 11. does NOT place the application in condition of allowance because applicant's argument is not persuasive:

Applicant argues that the amendment should be entered because it complies with requirements of 37 C.F.R. 1.116(b)(1). 37 C.F.R. 1.116(b)(1) states: "An amendment may be made canceling claims or complying with any requirement of form expressly set forth in a previous Office action". However, the rejection under section 112 required applicant to show how the first station verifies the hash of the intermediate key. The added requirements are related to decrypting the encrypted key. There is no indication on how the hash is verified. Therefore, the amendments to claims will not be entered.

Rejection under section 112:
As mentioned above, the amendments do not simplify the issue raised by the rejection under section 112. Accordingly, the rejection under section 112 is maintained.

Rejection under section 103:

Applicant makes a general allegation that Perlman and SSL protocol do not relate to distribution of session specific symmetric keys, or mutual authentication, or the use of a session key. However, SSL protocol creates secured communication between parties and distributes a symmetric session key between the parties to be used to secure the communication. A stated purpose of Perlman's invention is overcoming the shortcomings of the SSL protocol (see col. 2 lines 19-43). Perlman is clearly related to authentication as an application of key distribution. It is noteworthy that the word authentication only appears in the preamble of the claimed invention, as the preamble reads: "A method for producing ephemeral, symmetric encryption keys at a first station *for mutual authentication* and secure distribution of a random session-specific symmetric encryption key in a communication session with a second station, comprising:" SSL also mutually authenticates the parties before distributing the session keys, and therefore is clearly related to mutual authentication.

Applicant argues that Kelly does not teach a system for exchanging keys, and only teaches a system for exchanging passwords. However, Perlman is clearly related to exchanging and distributing keys. Also, a password is a shared secret useful for authentication. A key is also a shared secret used in authentication applications. Therefore, it would have been obvious to use Kelly's teachings to exchange keys.

Applicant further argues that the word mutual is not existing in Perlman. However, as mentioned before, SSL involves mutual authentication. Therefore, Perlman teaches mutual authentication in essence. It is also noteworthy that the claim language uses the word mutual authentication in the preamble only, and as an application, based on key distribution. Therefore, it is not clear how reference to mutual authentication in the preamble, distinguishes the invention from the prior art.

Applicant continues their argument based on the preamble, and states that Perlman does not describe a process for secure distribution of random session specific symmetric encryption keys. However, as mentioned before, Perlman describes distribution of random session specific symmetric encryption keys at least by its reference to SSL protocol, which clearly distributes symmetric keys for securing communication sessions.

Applicant further argues: "Examiner mistakenly uses this reference in Perlman as an example of ".., a plurality of exchanges executed for distributing the symmetric encryption key produced for use in the communication session."". However, Examiner's first bullet in paragraph 7.1. references SSL as teaching the subject of assigning a session key to establish a secure communication. The limitation of a plurality of exchanges for distributing symmetric encryption keys is taught by Perlman col. 5 line 5 to col. 6 line 57 and as described in the rejection. The option of using symmetric keys as an alternative to private/public key pairs is clearly suggested at Perlman col. 5 lines 68 and 69.

Applicant further argues that the limitation of: "associating, in the first station, a set of intermediate data keys, different from said session key, with said request for use in said plurality of changes" is not interpreted correctly to be met by Perlman column 5, lines 55-67. I support of their argument, applicant states: "The SSL protocol relied upon in the Office Action is used for distribution of a public key. A symmetric key used in that protocol, previously distributed in an unknown process and already in the possession of the second station, is delivered to the first station encrypted using the public key. (Perlman, column 2, line 19-24)." However, it is not clear how the cited paragraph of Perlman (col. 2 line 19-24) leads to such conclusion, or how that conclusion is related to Examiner's interpretation and rejection. Perlman col. 5 lines 26-32 clearly shows that an ephemeral symmetric key is encrypted using another symmetric key and sent from the first station to the second. This encrypted message includes the ephemeral key. The symmetric key to encrypt the ephemeral symmetric key is already established between the parties. Perlman teaches SSL as a protocol for establishing symmetric session keys. Therefore, Perlman teaches setting up a session key using SSL and the set up session key is used for encrypting the ephemeral symmetric keys. Therefore, Perlman meets the requirement of "associating, in the first station, a set of intermediate data keys, different from said session key, with said request for use in said plurality of changes".

Applicant continues with a list of alleged errors:

a. Applicant states Perlman keys are obliterated at the end of each session, but does not specify how this would be an error relative to the rejection of claims.

b. Applicant states a session key in Perlman is a key with life time that is exactly the session duration. Applicant then concludes that any key chosen by the second station is not truly ephemeral with respect to session time. First, it is not clear what is meant by "not truly ephemeral with respect to the session time. Second, it is not clear how this conclusion, even if considered valid, amounts to an error in rejection.

c. Applicant states: "However, in our claims, the intermediate data keys are used in a plurality of exchanges during a session for distribution of a symmetric key. Clearly, this is not the case in Perlman, where only one key pair is used in a session, distribution of the key is not described, and no key pair in the list is involved in any session using a different key pair."
However, it is not clear how the applicant determines a Perlman session, or concludes only one key pair is used in a session. A session could include a plurality of messages. The set ephemeral keys exchanged in Perlman may constitute a session.

d. Applicant states: "Once Perlman extrapolates the Fig. 3 algorithm to symmetric encryption keys - out of all steps in this algorithm, only the first and last steps can be really implemented." However, applicant does not provide any reason for such conclusion.

Applicant further continues: "Unlike Kelly, the present invention provides a protocol by which secret credentials are never required to be transferred over communication lines, either in clear text or in encrypted form." However, the instant application exchanges a shared secret between the two parties to verify receipt of a session key, and Kelly also shows verification of a session key based on a shared secret encrypted and exchanged between the two parties.

Applicant continues: "Although the claims recite encryption of a shared parameter, in the present invention, it is not the shared parameter that is verified in the plurality of exchanges. Furthermore, as is abundantly clear in the specification of the present application, the shared parameter recited in claim 1 need not be, and is preferably not, a secret client credential." Once again, Kelly teaches verification of a session key based on a shared secret encrypted and exchanged between the two parties, and therefore known in the art. This teaching, in combination with Perlman's teachings, makes the invention obvious to the one skilled in art. Applicant has not established any reason that shows Kelly teaches away from the claimed invention.

Applicant further argues against each sentence of Examiner's rationale set forth in page 5 of the Final office Action. Applicant's argument against each sentence of Examiner's rationale is based on their assumption that they have allegedly shown that each one of Examiner's statements is incorrect. However, as discussed above, none of applicant's arguments have been found persuasive. Therefore, applicant's argument against Examiner's rationale in page 5 is found non persuasive.

With regards to claim 23, 24, 26, 27, 29 and 30, applicant argues: "First, Applicant
points out that the present invention is not a cryptographic protocol for an iterated cryptosystem in which a cryptographically weak transformation is applied repeatedly to a message, so that the composed transformation is strong." However, as stated before, claim 23 is similar to claim 1, with an additional requirement of an iterative method, which involves application of a set of operations iteratively, each of those operations identical to one of the operations discussed as part of claim 1. Therefore, claim 23 is an iterative method, and the operations of each iteration is known in prior art. The operations in each iteration may be different than operations in DES or SKEY, but iteration improves the secrecy, and therefore the one skilled in art would be motivated to do so. It is also noted that applicant has not cited any reason for iteration in their invention that distinguishes it from what is cited in the prior art.

Applicant also states: 'Alternatively, Applicant demands under the provisions of MPEP 2144.03 Reliance on Common Knowledge in the Art or "Well Known" Prior Art, that the Examiner provide documentary evidence to support this unfounded conclusion." However, the cited references show that improving secrecy by iteration was known in the art.

Based on the above discussion, applicant's argument relative to allowability of the pending claims is found non persuasive.